Fig. 3 Scientific Articles from year 2009 to 2021

proceedings, and databases were investigated and explored in the area of homomorphic encryption. Scientific publications from Scopus, ACM Digital library, Springer Link, Sciencedirect, Google Scholar were selected based upon research questions given in Table 1. Fundamental studies in PHE, SWHE that function as cornerstones of homomorphic encryption were chosen first, followed by publications focused only on fully homomorphic encryption. A total of 1815 scientific papers were obtained using a database search with Keywords used for search as 'homomorphic encryption', and 'homomorphic encryption' or "medical" OR "healthcare" OR "bioinformatics" OR "EHR" OR "patient" OR "health" OR "medicine". Following the removal of duplicate documents, a total of 857 records were evaluated for title screening. After screening title total 194 articles were selected for abstract screening. In abstract screening 69 papers that were focused on homomorphic encryption based upon LWE, NTRU, Lattices, Integers, and HE papers focused mainly on healthcare and bioinformatics were selected. Other than that 19 important papers in PHE and SWHE (consider Fig. 4) were chosen for better understanding the concept of homomorphic encryption.

Inclusion and exclusion criteria

Scientific articles in journals, conferences proceedings, workshops published in the year range from Jan 2009 to Dec 2021 (Fig. 3) were considered. Other than that, Partial and Somewhat homomorphic encryption papers of the old era were also included to better understand the concept of homomorphic encryption. All quality research publications of fully homomorphic encryption after the Gentry FHE scheme were considered. Articles that were focused on the applicability of homomorphic encryption other than healthcare or bioinformatics were excluded.

Research questions

Prime objective of this review writing is to categorize the current literature on homomorphic encryption with its contributions in health informatics. This research study's end result is the identification and examination of homomorphic encryption methods in healthcare. A set of research questions are formulated for this systematic literature review in Table 1.

Background

The medical services industry is experiencing a digital revolution. Modernizing medical care has prompted another time of computerized wellbeing and health. Medical services information is gathered from different sources (e.g., sensors associated with patients) and stored in unique medical services clouds (e.g., private and public clouds). Also, the volume of agglomerated medical information is sufficiently enormous to qualify as "Big Data". As cloud medical services become a well-defined component in the medical services industry, there is a more critical requirement for safely sharing patient data across such dissimilar medical services clouds. Besides, with Accountable Treatment Organizations (ACOs) (e.g., medical service providers, specialists, clinics, and protection providers) collaborate to provide top-notch care, with demand for constant availability across cloud medical services higher than at any point in recent times. A disentangled patient-driven paradigm, in which patients can switch suppliers while still providing their data in a useful way for better diagnosis and treatment, and, in the long term, for enhanced global health, is appealing. As of now, medical care suppliers who have delicate patient information in private medical care clouds across the globe are reluctant to share that data on account of security and protection issues. As medical care suppliers move to the local area and public cloud-based administrations, a requirement for a secure connection between divergent medical care cloud increments. Moreover, security guidelines forced by Health Insurance Portability and Accountability Act (HIPAA) [6] and Health Information Technology for Economic and Clinical Health (HITECH) [7] place a cumbersome undertaking on medical care Information Technology (IT) framework to be agreeable with protection and security guidelines. Moreover, with arising Internet of Things (IoT) market and its mix in the vast information cloud stage, there is expanded worry about security and protection with the medical services cloud worldview. Many researchers contributed with their study in homomorphic encryption. Homomorphic encryption has three types: partial homomorphic encryption (PHE), somewhat homomorphic encryption (SWHE), and fully homomorphic encryption Fig. 5. PHE supports either